

REMARKS

The Office Action mailed November 13, 2007 has been carefully considered.

Reconsideration in view of the following remarks is respectfully requested.

Claim Status and Amendment of the Claims

Claims 1-4 are currently pending.

No claims stand allowed.

Claims 1-4 have been amended to further particularly point out and distinctly claim subject matter regarded as the invention. Support for these changes may be found in the specification, figures, and claims as originally filed.

Objections to the Specification

The abstract of the disclosure and the title of the invention stand objected to because of minor informalities.¹ A new ABSTRACT OF DISCLOSURE which is within 150 words is submitted herewith, and the title of the invention has been amended in accordance with the Examiner's suggestion. Accordingly, withdrawal of the objection to the Specification is respectfully requested.

Objections to the Claims

Claims 1-4 stand objected to for various informalities.² With this Amendment, Claims 1-4 have been amended accordingly. Withdrawal of the objection to the claims is respectfully requested.

¹ Office Action mailed November 13, 2007, ¶ 3.

With this Amendment it is respectfully submitted the claims satisfy the statutory requirements.

The 35 U.S.C. § 102 Rejection

Claims 1-4 stand rejected under 35 U.S.C. § 102(b) as allegedly being anticipated by Teng et al.^{3 4} This rejection is respectfully traversed.

According to the M.P.E.P., a claim is anticipated under 35 U.S.C. § 102(a), (b) and (e) only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference.⁵

Claim 1

Claim 1 as presently amended recites:

An apparatus for managing access for an extranet, comprising:
a plurality of domain web server, to which a plurality of users are subscribed,
an authentication and authorization (AA) server for managing access authentication and authorization for the domain web server,
an authority information storing module for storing authentication information and authorization information of the users, and
a user web browser interconnected with the AA server and the domain web server,
wherein the AA server comprises:
 an AA module for authenticating the users and setting Role values in an AA cookie of the authenticated user;
 an access control list (ACL) cache control module for synchronizing ACL caches of the respective domain web server with the AA server; an encryption module for encrypting the AA cookie to be given to each user; and
 a schema provider and user provider for providing an operation system independent of the authority information storing module,
wherein the domain web server comprises:
 an ACL cache which is delivered from the AA server;

² Office Action at ¶¶ 4-6.

³ U.S. Publication No. 2002/0138577 to Teng et al.

⁴ Office Action dated November 13, 2007 at ¶ 7.

⁵ Manual of Patent Examining Procedure (MPEP) § 2131. See also *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987).

an AA module for checking, by using the ACL cache, whether the user has authority to access a requested resource;
a decryption module for decrypting the encrypted AA cookies; and
a module for processing a resource request from the user web browser,
wherein the domain web server is configured to extract the Role values from the AA cookie of the user, extracts an access control entry (ACE) of the requested resource from the ACL cache, and grant an access authority to the user if the ACE of the requested resource exists in the extracted Role values.

The Examiner states,

... Tong discloses:

- **An apparatus for managing access for an extranet, comprising:** (Abstract and Claim 30, "An **apparatus** according to claim 24, wherein: said one or more processors are part of an **integrated identity and access system**.")) and (Par [0144], lines 7-11, "**Extranet and grant Extranet access** to many different companies. The entity setting up the Extranet is node 230. Each of the companies with Extranet access would have a node at a level below node 230."))

- **a plurality of domain web server, to which a plurality of users are subscribed,**

(Par [0479], "An Internet domain can reside on a single Web Server, or be distributed across multiple Web Servers. In addition, multiple Internet domains can reside on a single Web Server, or can be distributed across multiple Web Servers. In accordance with the present invention, the **Access System allows a user to satisfy the authentication requirements** of a **plurality of domains** and/or Web Servers by performing a single authentication.")) and (Par [0113], lines 1-8, "With **Group Manager 44**, companies (or other entities) can allow individual **users** to do the following: (1) self **subscribe to and unsubscribe from groups**, (2) view the groups that they are eligible to join or have joined, and (3) request subscription to groups that have access to the applications they need. Multi-step workflows can then define which users must obtain approval before being added to a group and which can be added instantly.").

- **an AA server for managing access authentication and authorization for the domain web server,**

(Par [0109], lines 16-19, "An administrator can be delegated any allowed degree of responsibility. For example, a company might decide that only IT staff can assign **application access**") and (Par [0161], lines 1-7, "Configure tab 416 allows a user to configure various options for **User Manger 42**. The user must have sufficient privileges to access Configure tab 416. The user can perform attribute **access control**, delegate administration, define workflows and set the search base. **Attribute access control** includes controlling who has view and modify permissions for each attribute.").

- **an authority information storing module, and a user web browser interconnected with the AA server and the domain web server, wherein the AA server comprises an AA module playing a role of authentication and authorization;**

(Par [0398], lines 1-12, "if a status check is not required, **Identity Server 40** exports the requested certificate to the user **via Web Server 20** (step 3434)... Certificate Authority 2084, as described above with reference to FIG. 59A. In some embodiments, Identity Server 40 also **stores** the retrieved real time certificate status and related **validation information**") and (Par [0161], lines 5-7, "**Attribute access control** includes controlling who has view and modify permissions for each attribute.").

- **an ACL cache control module for synchronizing ACL caches of the respective domain web server with the AA server;**

(Par [0352], lines 2-13, "servers that are equipped to communicate with each other in accordance with the present invention. Identity Server 1900 contains a **set of function modules 1904**. Each function module contains instructions for carrying out a program that may be called for by a request. Function module set 1904 communicates with a set of caches 1906. Caches in set 1906 contain data frequently used by function modules in set 1904. **The following caches are representative of those in set 1906:** (1) **Access Control Policy Cache**; (2) **System Specific Data Cache**; (3) **Workflow Definition Cache**; (4) **X Structure Cache**; (5) **Server Information Cache**; (6) **Application Information Cache**; and (7) **Master Audit Policy Cache**").

- **an encryption module for encrypting AA cookies to be given to the users;**

(Par [0155], lines 4-13, "**the user**, regardless of where it is stored and in what format. ... **the cookie is encrypted**").

- **and a schema provider and user provider for providing an operation system independent of the authority information storing module,**

(Par [0278], lines 4-9, "Some of these attributes are part of structural object class, while others are part of auxiliary object classes (or auxiliary object class schema)...").

- **wherein the domain web server comprises an AA module for checking, by using the ACL cache, whether the user accesses;**

(Par [0352], "FIG. 46 shows a block diagram of two identity servers that are **equipped to communicate** with each other in ... **function modules** in set 1904. The following caches are representative of those in set 1906: (1) **Access Control Policy Cache**; (2) **System Specific Data Cache**; (3) **Workflow Definition Cache**; (4) **X Structure Cache**; (5) **Server Information Cache**; (6) **Application Information Cache**; and (7) **Master Audit Policy Cache**").

- **an ACL cache which is delivered from the AA server;**

(Par [0106], " Access Server 34 provides authentication, authorization, auditing logging services.... Servers.").

- **a decryption module for decrypting the encrypted AA cookies; and a module for processing a resource request from the user web browser,**

(Par [0380], lines 5-8, "In another implementation, the user encrypts the request using a private key and certificate registration **module 2072** is able to decrypt...") and (Par [0433], lines 2-4, "requested resource is protected. In step 2630, **Web Gate 28** determines whether an entry for the requested resource is found in a **resource cache....** ").

- wherein the domain web server checks the user authority by using **ACL information, respectively, and produces the encrypted Role information cookie,**

(Par [0430], lines 10-16, "if the user has previously authenticated for a protected resource in the same domain, a valid authentication cookie is passed by browser 12 with the request in step 2550. The authentication cookie is intercepted by Web Gate in step 2552. If a valid cookie is received (step 2554), the method attempts to authorize the user in step 2556.").

- **this cookie signal being authenticated in the AA server 300, and, after authentication, Role, ACL, and ACE information is stored in the authority information storing module.**

(Par [0106], "The Access System includes Access Server 34, Web Gate 28, and Directory Server 36. Access Server 34 provides **authentication, authorization, auditing logging services... Web Servers.**") and (Col. [0097], lines 13-17, "The system decentralizes their administration by hierarchy delegating administrative **roles.**") and (Par [0381] Certificate registration **module 2072** forwards the automatic renewal ... to **Certificate Authority 2084** as a certificate signing request (step 2222). Certificate Authority... Certificate registration module 2072 updates the certificate in the data store...) and (Par [0107], lines 5-10, "The data elements of the **identity profile are called attributes,** The Identity Server includes three main applications, which effectively handle the identity **profiles and privileges of the user population...**") and (Par [0143], "Examples ...of **attributes stored** in a group identity profile include: owner, name, description, static members, dynamic member rule, subscription policies, etc Examples of attributes stored in a user organization identity profile include: owner, name, description, business category, address, country, etc. In other embodiments, less or more than the above-listed information is stored") and (Fig. 14, "provide list of proxies") and (Par [0177], "A **list of identified users** is then depicted on the substitute rights tab") "ACE" being all the "attributes stored".⁶

The Applicants respectfully disagree for the reasons set forth below.

The Applicants respectfully submit the terms "authentication" and "authorization" as disclosed in the present application, have separate and distinct meanings. In the context of embodiments of the invention as presently claimed, the purpose of "authentication" is to identify users. Whereas the purpose of "authorization" is to determine whether the user has authority to access a requested page and thus be granted access authority.

⁶ Office Action, pp. 3-8. (emphasis in original)

Teng et al. is directed towards the centralization of authentication and authorization.⁷

The Access server (34) of Teng et al. provides centralized authentication, authorization, and auditing services, but the Web server (18) of Teng et al. is unable to authorize users.⁸ However, as shown in FIGS. 5 and 6 of the present application, embodiments of invention as presently claimed are directed towards *decentralization* of authority management. The authentication is performed in the authentication and authorization (AA) server (300), but authorization (for example, referring the authority and grant the access authority) is performed in the each Web server (100).⁹ This difference is exemplified in several ways, as is discussed in more detail below.

In embodiments of the invention as presently claimed, Role values are stored in an AA cookie when for use in user authentication. The Role values stored in the AA cookie would be used when users are authorized to access protected resources. In Teng et al., cookie (3150) does not include information related to the authorization. Cookie (3150) of Teng et al. includes authentication-related information, but does not include authorization-related information.¹⁰

Furthermore, Uid cookie (360) of Teng et al. is for administrating user information and is used when accessing the Identity server (40). Because the functions of cookie (3150) and Uid cookie (360) of Teng et al. are different from the AA cookie of the invention as presently claimed, the rejection of Claim 1 under 35 U.S.C. § 102(b) is unsupported by the cited art of record and must be withdrawn.

⁷ See, e.g. Teng et al. at ¶¶ 97, 106, and 117; and FIG. 1.

⁸ See, e.g. Teng et al. at ¶ 117.

⁹ See, e.g. Specification at p. 6, 3rd and 4th paragraphs.

Additionally, Claim 1 recites in part a Web server comprising an access control list (ACL) cache(104). The ACL cache is memory space storing ACL information, and it is synchronized with AA server. The ACL is a list of access control entries (ACEs), which include authorization-related information. Whereas the caches of Teng et al. are in the Identity server (1900, 1902) and the Access server.¹¹ The Web server of Teng et al. lacks even a cache which stores authorization-related information.

Claim 1 as presently amended recites in part that the Web server is configured such that it could provide authorization by using the AA cookie and the ACL caches. In particular, Claim 1 recites in part that when the protected resources are accessed by a user, the Web server extracts the Role values from the AA cookie of the user, extracts an ACE of the requested resource from the ACL cache, and grants an access authority to the user if the ACE of the requested resource exists in the extracted Role values.

An example process of authorization is as follows. The Role information would be stored in the AA cookie when authentication is processed. ACE information, for example [R1=a.html, b.html, c.html] and [R2=d.html, e. html], is in the ACL Cache of Web server. Now, an authenticated user is requesting the Web server to access b.html which is protected. If R1 is in the AA cookie of the authenticated user, the Web server could authorize the authenticated user to access b.html. However, if the authenticated user does not have R1 in the AA cookie, Web server would deny the authenticated user to access b.html.

¹⁰ See, e.g. Teng et al. at ¶486; and FIG. 71.

¹¹ See, e.g. Teng et al., FIGS. 46 and 68.

On the contrary, the Web server of Teng et al. cannot authorize users. The Access server of Teng et al., not the Web server, checks the user authority and grants the access authority to users. Only the Access server of Teng et al. checks whether the user is authorized to access the protected resources.¹²

Additionally, because Teng et al. is directed towards centralized authorization, the Access server of Teng et al. checks the request signals received from all of the users and grants the authority. Therefore, Teng et al. is suitable only for an in-house intranet or a small-scale portal site, which has a small number of users and small amount of usage. Embodiments of the invention as presently claimed overcome problems of centralized authorization by using an AA cookie and an ACL cache.

With this Amendment, Claim 1 has been amended to make the above distinctions more clear. For the above reasons, the rejection of Claim 1 under 35 U.S.C. § 102(b) is unsupported by the cited art of record and the rejection must be withdrawn.

Claim 2

Claim 2 as presently amended recites:

A method of managing access for an extranet, performed in the apparatus which comprises the elements in claim 1, the method comprising the steps of:
an ACL initialization operation comprising:
 an AA module of a domain web server requesting the ACL cache control module of the AA server to synchronize an ACL; and
 the ACL cache control module referring the ACL from the authority information storing module and delivering the referred ACL data to the AA module of the domain web server;
an authorizing operation in authentication comprising:
 a user web browser accessing the domain web server;

¹² See, e.g. Teng et al. at ¶ 488-490; and FIG. 72.

the AA module of the domain web server confirming access authority of the user web browser;
the user web browser requesting the authentication from an AA module of the AA server;
the AA module of the AA server referring a schema provider to the authority;
the schema provider referring an authority information storing module to a site and delivering the referred result to a user provider; and
the user provider referring the authority information storing module to the user authority to make authentication, setting Role values in an AA cookie of the authenticated user, and transmitting the AA cookie to the user web browser; and
an authority referring operation comprising:
a user web browser requesting a page (URL) access from the domain web server;
the AA module of the domain web server checking whether the user has an authority to access the requested page by comparing the Role values in the AA cookie and ACEs of the ACL cache; and
the resource request processing module processing the requested page (URL) and responses to the user web browser by sending a processed result.

The Examiner states,

... the rejection of Claim 1 is incorporated and further Teng discloses:

- **A method of managing access for an extranet, performed in the apparatus which comprises the elements in claim 1, the method comprising the steps of: a user web browser accessing a domain web server, an AA module of the domain web server confirming access authority of the user web browser,**

(Par [0398], lines 1-12 "If a status check is not required, Identity Server 40 exports the requested certificate to the user via **Web Server 20** (step 3434).... Certificate Authority 2084, as described above with reference to FIG. 59A. In some embodiments, Identity Server 40 also stores the retrieved real time certificate status and related **validation information**") and (Par [0161], lines 5-7, "**Attribute access control** includes controlling who has view and modify permissions for each attribute.") and (Par [0113], lines 1-8, "With **Group Manager 44, companies** (or other entities) can allow **individual users to do the following:... access to the applications** they need. Multi-step workflows can then define which users must obtain **approval** before being added to a group and which can be added instantly.").

- **the user web browser requesting the authentication from the AA module of the AA server, the AA module of the AA server referring a schema provider to the authority,**

(Par [0109], lines 16-19, "An administrator can be delegated any allowed degree of responsibility. For example, a company might decide that only IT staff can assign **application access**") and (Par [0161], lines 1-7, "Configure tab 416 allows a user to configure various options for **User Manger 42**. The user must have sufficient privileges to access Configure tab 416. The user can perform attribute **access control**, delegate administration, define workflows and set the search base. **Attribute access control** includes controlling who has view and modify

permissions for each attribute.") and (Par [0278], lines 4-9, "Some of these attributes are part of structural object class, while others are part of auxiliary object classes (or auxiliary object class **schema**)...").

- **the schema provider referring an authority information storing module to a site and delivering the referred result to a user provider,** (Par [0233], "... **storing** a list of the groups in a file, **providing identifications of the groups** to another process, etc. In one example, **the access system** requests that the Identity System determine a user's groups so **that the access system can authorize a user to access** a resource based on membership in a particular group.").

- **and the user provider referring the authority information storing module to the user authority to make authentication and set user authority, and transmitting the information to the user web browser.** (Par [0106], lines 1-8, "The Access System includes Access Server 34, Web Gate 28, and Directory Server 36. Access Server 34 provides **authentication, authorization**, auditing logging services. It further provides for identity profiles to be used across multiple domains and Web Servers from a single web-based authentication (sign-on). Web Gate 28 acts as an interface between Web Server 18 and Access Server 34.") and (Par [0478], lines 16-24, "in one embodiment, **Web Gate 28 transmits** a flag with all POST requests forwarded to Access Server...").¹³

The Applicants respectfully disagree for the reasons set forth below.

Claim 2 is a method performed in the apparatus comprising the elements of Claim 1.

Claim 1 being allowable, Claim 2 must also be allowable for at least the same reasons as Claim

1. Additionally, Claim 2 as presently amended recites in part multiple operations not disclosed by Teng et al., such as an access control list (ACL) initialization operation, an authorizing operation in authentication, and an authority referring operation. Teng et al. fails to disclose ACL cache-initialization, ACL cache-synchronization, and an AA cookie in which authorization-related information is stored. Furthermore, the Web server of Teng et al. cannot provide authorization.

¹³ Office Action, pp. 8-10. (emphasis in original)

Claims 3 and 4

Claims 3 and 4 depend from Claim 2. Claim 2 being allowable, Claims 3 and 4 must also be allowable for at least the same reasons as for Claim 2.

In view of the foregoing, it is respectfully asserted that the claims are now in condition for allowance.

Conclusion

It is believed that this Amendment places the above-identified patent application into condition for allowance. Early favorable consideration of this Amendment is earnestly solicited.

If, in the opinion of the Examiner, an interview would expedite the prosecution of this application, the Examiner is invited to call the undersigned attorney at the number indicated below.

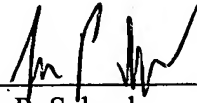
The Applicant respectfully requests that a timely Notice of Allowance be issued in this case.

Please charge any additional required fee or credit any overpayment not otherwise paid or credited to our deposit account No. 50-1698.

Respectfully submitted,

THELEN REID BROWN
RAYSMAN & STEINER LLP

Dated: March 13, 2008



John P. Schaub
Reg. No. 42,125

THELEN REID BROWN RAYSMAN & STEINER LLP
P.O. Box 640640
San Jose, CA 95164-0640
Tel. (408) 292-5800
Fax. (408) 287-8040